Attorney's Docket No.: 10559-148001 / P7973

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Ulhas S. Warrier et al.
Serial No. : 09/539,928
Filed : March 31, 2000
Title : NETWORK SESSION MANAGEMENT

Art Unit : 2134
Examiner : Ellen C. Tran

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION OF ULHAS S. WARRIER UNDER 37 C.F.R. § 1.131

I, Ulhas S. Warrier, currently residing at 16840 NW Eastmoreland Ct., Beaverton, OR 97006, do hereby declare as follows:

1. I am a co-inventor, along with N. Prakash Iyer, of the invention claimed in the above-identified patent application.

2. Prior to January 12, 2000, N. Prakash Iyer and I invented the subject matter of the claims of this patent application while being employees of Intel Corporation, currently having a place of business at 2200 Mission College Blvd., Santa Clara, CA 95052. At least as early as January 12, 2000, we conceived of and proceeded to diligently reduce to practice the invention claimed in the above-referenced patent application.

3. This is evidenced by a written invention disclosure, which was the basis of the above-referenced patent application, and which we prepared for submission to patent counsel at least as early as January 12, 2000. The invention disclosure contents describe the invention, and a redacted copy of the invention disclosure is included along with this declaration. The invention disclosure form itself is considered confidential to Intel Corporation, and each date on the form supports statement 2 above.

CERTIFICATE OF TRANSMISSION BY FACSIMILE

I hereby certify that this correspondence is being transmitted by facsimile to the Patent and Trademark Office on the date indicated below.

September 16, 2005
Date of Transmission

Veronica Whalen
Signature

Veronica Whalen
Typed or Printed Name of Person Signing Certificate

Applicant : Ulhas S. Warrier et al.
Serial No. : 09/539,928
Filed : March 31, 2000
Page : 2 of 2

Attorney's Docket No.: 10559-148001 / P7973

4. Moreover, after conception, and prior to January 12, 2000, we worked diligently with patent attorneys who were members of Fish & Richardson P.C. to prepare a patent application that described the conceived invention. After this diligent preparation work, the above-referenced application was filed on March 31, 2000.

5. The U.S. Patent No. 6,539,483 B1 cited by the U.S. Patent and Trademark Office is issued from the U.S. Application 09/481,831 filed on January 12, 2000, and no priority filing information is included in issued U.S. Patent No. 6,539,483 B1. Therefore, the evidence and statement of facts described in this declaration provides a prima facie showing that the invention date of our claimed invention was at least prior to the earliest priority date of the U.S. Patent No. 6,539,483 B1.

6. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Respectfully submitted,

Date: 8/8/05

Ulhas S. Warrier

10488775.doc

[redacted]

DATE: 10/6/99

OCT 11 1999

[redacted]

Inventor: Warrier (Last Name) Ulhas (First Name) S (Middle Initial)

[redacted]

Citizenship: India

[redacted]

Home Address: 16840 NW Eastmoreland Ct.

City Beaverton State OR Zip 97006 Country USA

[redacted]

Inventor: Iyer (Last Name) Prakash (First Name) (Middle Initial)

Phone (503) 264 1815

Citizenship: India

[redacted]

Home Address: 16617 NW Avondale Drive

City Beaverton State OR Zip 97006 Country USA

[redacted]

Title of Invention: Method for policy-driven dynamic network re-configuration of remote system in a trusted manner, based on context-specific information.

[redacted]

Virtual Private Networking (VPN)

RECEIVED

OCT 12 1999

Remote Access, Policy distribution, Policy enforcement, packet filters, consumer firewalls,

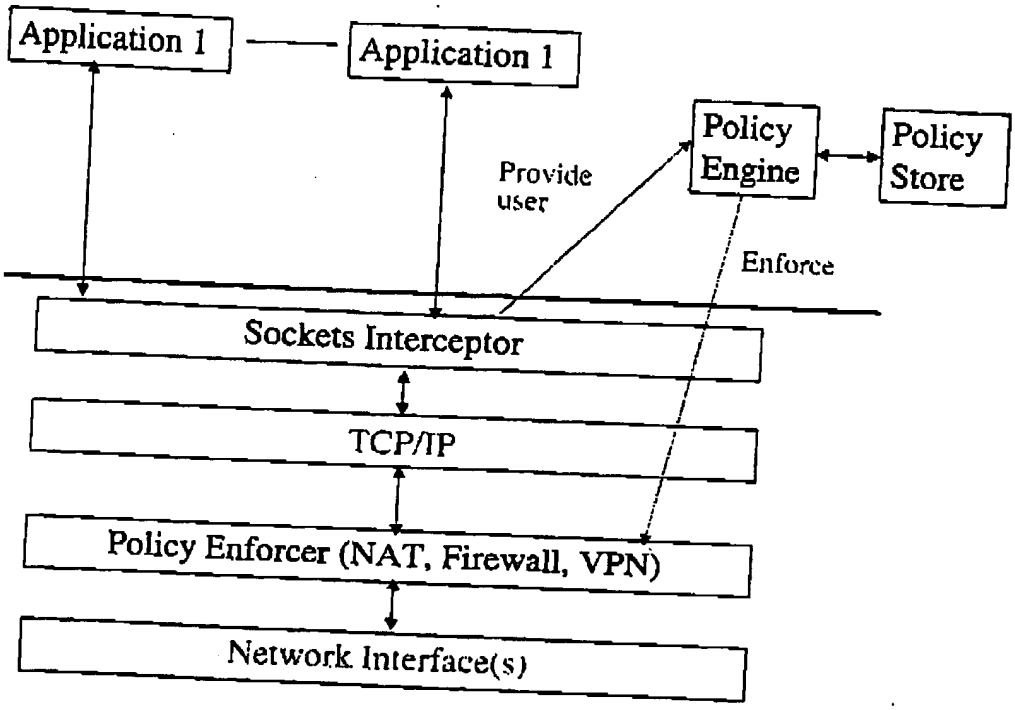
[redacted]

INTEL LEGAL TEAM

[redacted]

REDACTED

Illustration



[redacted]

[redacted]

Describe in detail what the components of the invention are and how the invention works.
Remote access VPNs – accessing a corporate LAN securely over the public Internet from a SOHO is an application that is gaining widespread deployment. Security technologies such as IPSEC combined with end-to-end QoS are fueling this class of applications. A second trend is the emergence of high-speed last mile access technologies for consumer networks such as ADSL and cable modems. These AOAC technologies also significantly increase the vulnerability of the consumer network to sustained network attacks. The consumer network could also become a conduit for a hacker on the public Internet to access sensitive information on a corporate network during a VPN session. It is obvious then, that IT administrators want to impose restrictions on network access privileges of the remote system during a VPN session. For e.g., in a setup where the corporate network is accessed from a home network using VPN, the gateway might decide to allow the client access to the printer at home but not to the public Internet.

The invention proposes a method for dynamic reconfiguration of network resource usage by the remote system. The nature of reconfiguration is determined by policies.

The delivery of the policies will be done using the same mechanism the remote access application (VPN) employs to retrieve security parameters for securing the tunnel. This means that policies are delivered to remote system in a trusted manner – i.e., without being compromised by mid-stream elements and host based software. Also, the policies are delivered just prior to establishment of a secure connection, making it dynamic in nature. We do not propose specific solutions for policy distribution itself.

The policies will be tailored to control network behavior of a single system. This might involve fine-grained filter specifications for e.g., controlling flow on certain network interfaces (disallow IP forwarding), filtering packets based on certain protocols/ports/subnets.

Enforcement of policy involves reconfiguring the network stack and dynamic activation of new components (filters). Network flows are tracked by various factors e.g., type (local or remote and transiting), network interfaces, destination network address, source (application, proxy, user etc). The assigned policy is applied to these flows for the period when the remote system is subscribing to the network of the gateway that administered the policy.

The invention uses unified network stack information to enforce these context-based policies i.e., an aggregation of information across various layers (session through data link) of a network stack. The combination of application and/or user context to network flows enables fine-grained control of network resources.

Describe advantage(s) of your invention over what is done now.

Currently, policies are fairly limiting. IT departments require that network browsing in the clear (not using a secure tunnel), access to the internet from internal nodes (if the VPN client is also a NAT gateway) and other home networking functions be disabled during the VPN session. The method proposed above allows the administrator to change this policy easily (making it dynamic) and also to enforce context (for e.g., user/applications) specific policies. These policies can be implemented without user intervention (other than for specification of local policies). The invention also embodies merging of local (remote user specified) and global (VPN administrator specified) policies transparent to applications.

Attorney's Docket No.: 10559-148001 / P7973

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Ulhas S. Warrier et al.
Serial No. : 09/539,928
Filed : March 31, 2000
Title : NETWORK SESSION MANAGEMENT

Art Unit : 2134
Examiner : Ellen C. Tran

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION OF N. PRAKASH IYER UNDER 37 C.F.R. § 1.131

I, N. Prakash Iyer, currently residing at 16617 NW Avondale Drive, Beaverton, OR 97006, do hereby declare as follows:

1. I am a co-inventor, along with Ulhas S. Warrier, of the invention claimed in the above-identified patent application.

2. Prior to January 12, 2000, Ulhas S. Warrier and I invented the subject matter of the claims of this patent application while being employees of Intel Corporation, currently having a place of business at 2200 Mission College Blvd., Santa Clara, CA 95052. At least as early as January 12, 2000, we conceived of and proceeded to diligently reduce to practice the invention claimed in the above-referenced patent application.

3. This is evidenced by a written invention disclosure, which was the basis of the above-referenced patent application, and which we prepared for submission to patent counsel at least as early as January 12, 2000. The invention disclosure contents describe the invention, and a redacted copy of the invention disclosure is included along with this declaration. The invention disclosure form itself is considered confidential to Intel Corporation, and each date on the form supports statement 2 above.

CERTIFICATE OF TRANSMISSION BY FACSIMILE

I hereby certify that this correspondence is being transmitted by facsimile to the Patent and Trademark Office on the date indicated below.

September 16, 2005
Date of Transmission

Veronica Whalen
Signature

Veronica Whalen
Typed or Printed Name of Person Signing Certificate

Applicant : Ulhas S. Warrier et al.
Serial No. : 09/539,928
Filed : March 31, 2000
Page : 2 of 2

Attorney's Docket No.: 10559-148001 / P7973

4. Moreover, after conception, and prior to January 12, 2000, we worked diligently with patent attorneys who were members of Fish & Richardson P.C. to prepare a patent application that described the conceived invention. After this diligent preparation work, the above-referenced application was filed on March 31, 2000.

5. The U.S. Patent No. 6,539,483 B1 cited by the U.S. Patent and Trademark Office is issued from the U.S. Application 09/481,831 filed on January 12, 2000, and no priority filing information is included in issued U.S. Patent No. 6,539,483 B1. Therefore, the evidence and statement of facts described in this declaration provides a prima facie showing that the invention date of our claimed invention was at least prior to the earliest priority date of the U.S. Patent No. 6,539,483 B1.

6. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Respectfully submitted,

Date: August 8th 2005

Prakash Iyer

N. Prakash Iyer

10488776.doc

[redacted]

DATE: 10/6/99

OCT 1 1 1999

[redacted]

Inventor: Warrier Ulhas S
Last Name First Name Middle Initial

[redacted]

Citizenship: India

[redacted]

Home Address: 16840 NW Eastmoreland Ct.

City Beaverton State OR Zip 97006 Country USA

[redacted]

Inventor: Iyer Prakash
Last Name First Name Middle Initial

Phone (503) 264 1815

Citizenship: India

[redacted]

Home Address: 15617 NW Avondale Drive

City Beaverton State OR Zip 97006 Country USA

[redacted]

Title of Invention: Method for policy-driven dynamic network re-configuration of remote system in a trusted manner, based on context-specific information

[redacted]

Virtual Private Networking (VPN)

RECEIVED

Remote Access, Policy distribution, Policy enforcement, packet filters, consumer firewalls.

OCT 1 2 1999

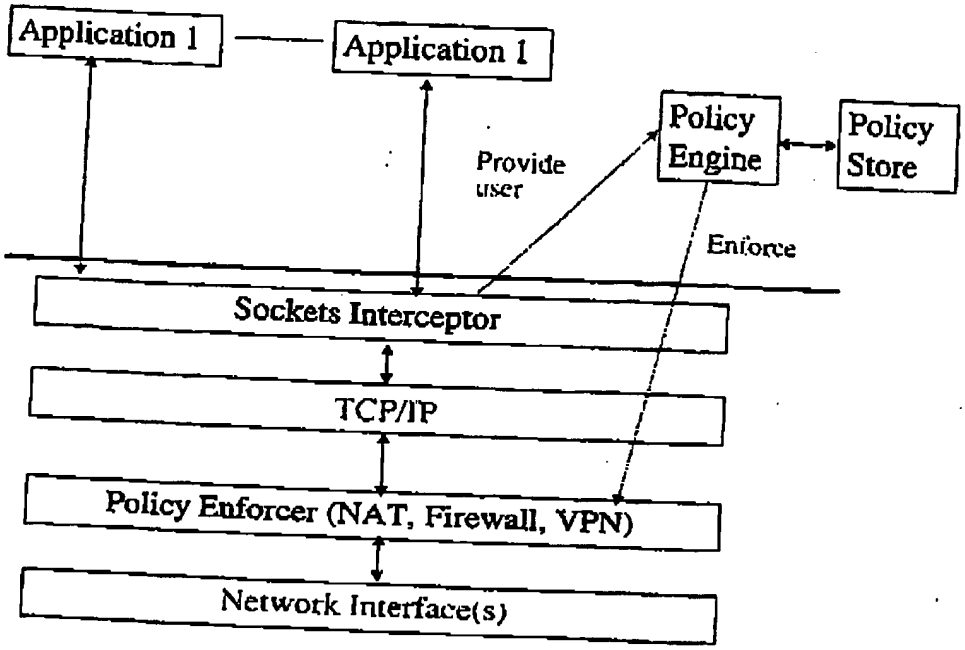
INTEL LEGAL TEAM

[redacted]

REDACTED

[redacted]

Illustration



[redacted]

[redacted]

[redacted]

Describe in detail what the components of the invention are and how the invention works.
Remote access VPNs – accessing a corporate LAN securely over the public Internet from a SOHO is an application that is gaining widespread deployment. Security technologies such as IPSEC combined with end-to-end QoS are fueling this class of applications. A second trend is the emergence of high-speed last mile access technologies for consumer networks such as ADSL and cable modems. These AOAC technologies also significantly increase the vulnerability of the consumer network to sustained network attacks. The consumer network could also become a conduit for a hacker on the public Internet to access sensitive information on a corporate network during a VPN session. It is obvious then, that IT administrators want to impose restrictions on network access privileges of the remote system during a VPN session. For e.g., in a setup where the corporate network is accessed from a home network using VPN, the gateway might decide to allow the client access to the printer at home but not to the public Internet.

The invention proposes a method for dynamic reconfiguration of network resource usage by the remote system. The nature of reconfiguration is determined by policies.

The delivery of the policies will be done using the same mechanism the remote access application (VPN) employs to retrieve security parameters for securing the tunnel. This means that policies are delivered to remote system in a trusted manner – i.e., without being compromised by mid-stream elements and host based software. Also, the policies are delivered just prior to establishment of a secure connection, making it dynamic in nature. We do not propose specific solutions for policy distribution itself.

The policies will be tailored to control network behavior of a single system. This might involve fine-grained filter specifications for e.g., controlling flow on certain network interfaces (disallow IP forwarding), filtering packets based on certain protocols/ports/subnets.

Enforcement of policy involves reconfiguring the network stack and dynamic activation of new components (filters). Network flows are tracked by various factors e.g., type (local or remote and transiting), network interfaces, destination network address, source (application, proxy, user etc). The assigned policy is applied to these flows for the period when the remote system is subscribing to the network of the gateway that administered the policy.

The invention uses unified network stack information to enforce these context-based policies i.e., an aggregation of information across various layers (session through data link) of a network stack. The combination of application and/or user context to network flows enables fine-grained control of network resources.

Describe advantage(s) of your invention over what is done now.

Currently, policies are fairly limiting. IT departments require that network browsing in the clear (not using a secure tunnel), access to the internet from internal nodes (if the VPN client is also a NAT gateway) and other home networking functions be disabled during the VPN session. The method proposed above allows the administrator to change this policy easily (making it dynamic) and also to enforce context (for e.g., user/applications) specific policies. These policies can be implemented without user intervention (other than for specification of local policies). The invention also embodies merging of local (remote user specified) and global (VPN administrator specified) policies transparent to applications.

[redacted]